AMENDMENTS TO THE SPECIFICATION:

Page 1, before line 3, insert the following as separate paragraphs:

--BACKGROUND OF INVENTION

1. Field of Invention--.

Page 1, before line 6, insert the following as a separate paragraph:

--2. Description of Related Art--.

Page 1, before line 19, insert the following as a separate paragraph:

--BRIEF DESCRIPTION OF THE INVENTION--.

Please amend the paragraph beginning at page 1, line 19, as follows:

According to a first aspect of the present invention, there is provided a method of distributing ~~digitially~~ digitally encoded data, comprising:

dividing said data into a multiplicity of frames,

encrypting said frames,

distributing multiple copies of the said data frames to a multiplicity of users,

communicating a seed value for key generation to respective secure modules located at each of the multiplicity of users,

decoding the data frames at respective users using keys derived from the seed value communicated to the secure module,

passing a control message to the secure module at a selected one or more of the multiplicity of users,

B3

at the or each selected user, in response to the said control message,

controlling the availability of keys generated from the said seed value, thereby selectively controlling access by the users to the said data.

Please amend the paragraph beginning at page 2, line 5, as follows:

B4

The method of the present invention provides full and effective control of access by users to data, without imposing heavy communication overheads. This is achieved by dividing the data item into frames, individually encrypting the frames with a series of keys, and using a controlled secure module at the customer location to generate the corresponding series of keys required to decrypt the received data. The secure module is controlled to ~~limlt~~ limit the availability of the keys. For example, an ~~intial~~ initial set-up message to the secure module may instruct it only to generate a limited number of keys, say one hundred. If the user subsequently pays to extend their subscription, then a further control message may be sent to the secure module to allow the generation of further keys from the existing seed value.

Please amend the paragraph beginning at page 2, line 15, as follows:

The invention includes, but is not limited to, data communications systems in which the frames or "ADU's" are communicated over, e.g., a federated public data network such as the Internet. It also encompasses systems in which the step of

communicating ADU's is carried out, e.g., by physically distributing a data carrier such as a CD-ROM containing the ADU's. The data on the distribution medium may be separated into frames each with a sequence number and each encrypted with a different key. During reading of data from the data carrier the ~~securme~~ secure module would generate keys, and this may be done off-line. An on-line connection may still be required, e.g. in order to request a receipt and for transmission of a response to such a request.

Please amend the paragraph beginning at page 4, line 30, as follows:

According to a second aspect of the present invention, there is provided a data communications system comprising:

a) a remote data source arranged to output a plurality of frames;

b) encryption means for encrypting the plurality of frames with different respective keys;

c) a communications channel arranged to distribute multiple copies of the encrypted data frames;

d) a multiplicity of customer terminals arranged to receive from the communications channel respective copies of the encrypted data frames;

e) a key generator located at a customer terminal and programmed to generate from a seed value keys for use in decrypting data frames:

f) key control means connected to the key generator, the key control means comprising:

an interface for receiving control messages; and

control means responsive to the said control messages and arranged to control the ~~availabiltiy~~ availability to the user of keys generated from the seed value; and

g) decryption means connected to the key generator and arranged to decrypt the data frames received at the customer terminal from the communications channel.

B5

Please amend the paragraph beginning at page 5, line 16, as follows:

According to another aspect of the present invention, there is provided a method of distributing ~~digitially~~ digitally encoded data, comprising

a) dividing said data into a multiplicity of frames,

b) encrypting said frames,

c) marking frames with a frame type field,

d) communicating said data frames to a user,

~~d~~e) communicating a seed value for key generation to the user,

~~e~~f) decoding the data frames at the users using keys derived from the seed value, and

~~f~~g) generating and storing receipts for said data frames, said frames including frame type data from the frame type field.

Page 5, before line 31, insert the following as a separate paragraph:

B6

--BRIEF DESCRIPTION OF THE DRAWINGS--.

Page 6, before line 18, insert the following as a separate paragraph:

B7 --DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS--.

Please amend the paragraph beginning at page 7, line 1, as follows:

B8 At each customer terminal, incoming data frames are processed using a secure module 4. As described in further detail below, the secure module 4 generates a sequence of keys corresponding to those used originally to encrypt the data frames. The number of keys to be generated in a given session are determined by a contract between the user and the operator of the data server. For example, in the case of video-on-demand, the user might select program material, in response to which the server identifies the number of keys required to ~~decrpt~~ decrypt all the frames in the program~~me~~, and the cost of the program~~me~~. In return for payment from the user, the server sends the seed value for the key, together with a control instruction for the secure module to generate the required number, e.g. one hundred, of the keys. The keys may be passed out to the main processor of the customer terminal to allow the data to be decrypted. Alternatively, the secure module itself may carry out the step of decryption. In either case, the secure module stores a record of the keys generated. This record may comprise, for example, a count of the total number of keys issued in the course of a session, together with a session ID and a record of the time of the session.

Please amend the paragraph beginning at page 7, line 17, as follows:

During the course of the session, control signals may be sent to modify the access rights of the customer. For example, the user might choose to quit a program at an early

stage and to gain a refund. This is effected by transmitting from the data server a data frame which contains, in addition to the data itself, a control message including the identity of the particular customer or group of customers whose access rights are to be modified. The control message may include a simple "stop" flag which, when set causes the secure module to cease releasing keys. Possible formats for the communication of control signals are discussed in further detail below with respect to Figures 10A and 10B. Conversely, the user might choose to view additional programme material, in which case a control message may be sent to the secure module to increase the number of keys to be generated e.g. from 100 to 200. Other changes in status are also possible. The frames may include a meta-data field which may be used to distinguish, for example, between different classes of subscriber. For example, subscribers might be divided into gold, silver and bronze classes, with gold users having access to data frames having meta-data values m1, m2 or m3, silver users having access to m1 or m2, and bronze users having access to m1 only. In return for payment during the course of a session, the user might upgrade their subscription e.g. from bronze to silver, and thereby gain access to programme material carried in frames with m2 meta-data values in addition to material carried in frames with m1 metadata values. The change is effected by the data server transmitting a control message to the secure module mandating key generation for m2 frames in addition to m1 frames.

Please amend the paragraph beginning at page 8, line 25, as follows:

Figure 2 shows the principal functional components of the customer terminal relevant to the present invention. A network interface 22 communicates data frames to and from the data network. The data frames pass from the interface 22 to a secure module 23. The secure module 23 has sub modules comprising a decryption module D_z a key generation module K and a secure store S. The key generation module passes a series of keys to the decryption module which decrypts a series of data frames received from the interface 22 and passes these to an application layer module 24. This carries out further processing and passes the resulting data to an output device, which in this example is a video display unit VDU 25. In a preferred implementation, the interface 22 may be embodied in hardware by an ISDN modem and in software by a TCP-IP stack. The secure module 23 may be, for example, a smartcard which is interface to the customer terminal via a PCMCIA socket. The smartcard may use one of a number of standard data interfaces such as the Java card API (application programmer's interface) of Sun Microsystems, or the Microsoft smartcard architecture. Alternatively, the secure module may be embodied by a PCI cryptographic co-processor card such as that available commercially from IBM.

B9

Please amend the paragraph beginning at page 22, line 1, as follows:

~~CLAIMS~~What is claimed is:.